CYBER AND DIGITAL OPERATIONAL RESILIENCE

ANNELI TUOMINEN

Member of the Supervisory Board – European Central Bank

Upgrading banks' capacity to deal with digital risks

Digitalisation is improving banks' efficiency, but it is also bringing about threats to their operational resilience. Such threats have been compounded by escalating geopolitical tensions, which have been associated with the rising number of cyberattacks on banks in recent years. The ECB has long recognised banks' operational resilience as a key area for improvement in the digital age. In recent years we have conducted a number of initiatives to help banks meet the challenges in this domain, including targeted reviews and on-site inspections on information technology security and outsourcing, as well as a cyber resilience stress test. More recently, our work in this field has been supported by a new EU regulation designed to keep digital risks in the financial sector in check: the Digital Operational Resilience Act (DORA), which came into effect in January 2025. I will now outline the supervisory benefits which this regulation has brought about so far and highlight the work still to be done in order to strengthen banks' capacity to deal with digital risks.

A growing focus on change management risk

First, DORA has improved our supervisors' ability to detect the operational information and communications technology (ICT) disruptions which banks routinely face, by establishing a broader reporting framework that is no longer limited to cyber incidents. With this new framework in place, we could see that 38% of the major incidents reported by banks in 2025 had "IT change" as their root cause. The growing number of ICT projects undertaken by banks and the complexities of running their operations effectively are contributing to exposing weaknesses in banks' change management processes and related controls. So while the silver lining is that there is a growing awareness among banks on the need to embrace new technologies and modernise their ICT infrastructure, it is also necessary to strengthen processes and controls so that banks can meaningfully reduce unplanned downtime in their ICT networks. This will be a key focus of supervisory attention for the ECB.

Increased oversight of third-party dependencies

Second, DORA has enabled our supervisors to have a better handle on banks' third-party dependencies. This aspect is particularly important as banks' reliance on a handful of third parties offering cloud services has been increasing sharply in recent years, as proxied by the growing weight of cloud service-related expenses in banks' total IT budget (rising from around 4% in 2021 to 17% in 2025). DORA requires financial institutions to assess and monitor third-party risks, establish clear contractual agreements and maintain strict controls over third-party arrangements. However, the experience thus far suggests that some banks are lagging behind when it comes to meeting these requirements, particularly in areas such as contract renegotiations with third-party providers and business continuity planning. We are therefore impressing on banks the need for them to close the remaining gaps promptly, which we will check through our on-site campaign on ICT third-party risk management. Moreover, to help keep in check the risks that critical ICT third-party service providers could pose to the broader financial sector, DORA introduces a comprehensive oversight framework for such parties at EU level. This framework, led by the three European Supervisory Authorities and to which the ECB is contributing through a team of dedicated staff, has been fully operational since January 2026, covering a total of 19 critical third-party service providers. Going forward, aspects such as subcontracting and how critical ICT services are provided to financial institutions will be a key point of attention of the oversight framework, with a view to preventing potential systemic impacts arising from service disruptions.

Ethical hacking and adapting to new technologies

Third, DORA requires certain types of banks designated as systemically important at either the global or domestic level to perform, at least once every three years, advanced security testing using external "ethical hackers" who will try to compromise their IT systems. Unlike traditional tests that look for technical vulnerabilities in specific applications, this threat-led penetration testing (TLPT) replicates the tactics, techniques and procedures of real world threat actors to test banks' live systems. Thanks to such tests, banks will be able to learn how to enhance their cyber resilience strategy, and the test outcomes will inform banks' and supervisors' holistic view on banks' cyber posture. The ECB will be responsible for managing these TLPTs for directly supervised entities and has published a dedicated guide[1] to explain how it intends to implement TLPT in accordance with DORA. The first three-year cycle of tests has already started, and more than 80 banking groups have been notified.

Looking ahead, the common challenge for banks and their supervisors stemming from the new DORA framework is to keep abreast of technological innovation, enabling banks to continue to exploit the benefits of such technologies while fending off the risks that these might pose and allowing supervisors to engage in meaningful dialogue with their supervised entities.

1. *https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guide202511.en.pdf*

SANTA PURGAILE
Deputy Governor – Bank of Latvia

One year after DORA: Implementation Challenges and Insights

One year has passed since the Digital Operational Resilience Act (DORA) entered into force, marking a significant milestone for the European financial sector. DORA has reshaped the regulatory landscape for ICT risk management, operational resilience, and cyber security, aiming to harmonize requirements across the EU and strengthen the sector's ability to withstand, respond to, and recover from digital disruptions.

Prior to DORA's application, Latvia had already had a well-established national-level regulatory framework governing key areas such as IT system governance, business continuity planning, recovery and testing of continuity measures, incident reporting, and outsourcing arrangements. This local regulation applied to financial institutions and provided a solid foundation for operational and ICT risk management. DORA applies to all market participants, regardless of size, as digital operational resilience is a prerequisite for trust and stability in financial markets. At the same time, proportionality remains essential. For very small entities with limited risk exposure and minimal systemic impact, simplified national-level requirements continue to apply.

As a result, for large and well-established market participants, particularly in the banking sector, DORA did not represent a conceptual shift. While implementation required additional efforts, in terms of documentation and standardization, these institutions were already familiar with most core requirements. In contrast, non-banking sector participants faced significantly greater challenges. DORA revealed practical challenges, as many market participants struggled with the creation and maintenance of outsourcing registers, the mapping of ICT dependencies, and the necessary changes to internal systems for incident reporting.

A clear difference in maturity levels became visible across the market. Some firms had limited experience with formal ICT governance frameworks, structured incident classification, or comprehensive outsourcing registers. This gap required substantial investments in governance, risk assessment capabilities, and internal controls.

Cyber resilience has long been a core focus of supervisory activities, predating the introduction of DORA. Over the years, all banks have updated their business continuity plans, strengthened recovery capabilities, and enhanced their ICT risk management frameworks in response to evolving threats. The proposals under the Digital Omnibus Package further support these efforts by improving regulatory coherence.

One year after DORA, uneven market maturity shaped the main challenges of digital resilience.

In recent years, supervisors have observed new and increasingly complex risk drivers, including heightened cyber threats, systemic dependencies, and concentration risks. Latvia, in particular, has been very active in identifying and regulating critical financial services by National level legislation through the imposition of stricter resilience and continuity requirements on large, important players. These measures complement DORA and reinforce cyber resilience.

Looking ahead, the cyber threat landscape is rapidly evolving due to increasing digitalization, geopolitical tensions, hybrid threats, and the growing use of AI. Geopolitical risks require further analysis and continuous adaptation of supervisory tools. A particularly important concern is the growing dependency of European financial institutions on third-party ICT service providers, many of which are located outside the EU. These dependencies can create concentration risks and expose institutions to vulnerabilities that are not always fully within their control. Continuous supervisory dialogue, further guidance, and enhanced cooperation at the EU level will be crucial to address these emerging risks effectively.

Technologies such as artificial intelligence, advanced security solutions, and monitoring tools can significantly enhance cybersecurity risk management. While AI can unfortunately also be exploited by attackers, it offers powerful defensive capabilities when used responsibly. AI-driven tools can improve threat detection, anomaly identification, and incident response by analysing large volumes of data more efficiently than traditional methods.

From a supervisory perspective, AI is valuable. Latvijas Banka actively uses AI-based solutions to strengthen our supervisory capabilities and enhance oversight processes. When combined with human expertise, and clear accountability, advanced technologies can play a decisive role in strengthening cyber resilience across the financial sector.

PETER E. STORGAARD

Assistant Governor and Head of Financial Stability Department – Danmarks Nationalbank

Ensuring critical financial functions for society amid evolving cyber risks

Over recent years, the cyber threat landscape has intensified primarily due to growing geopolitical tension that has altered both the intentions and behavior of hostile actors. The financial sector now operates in an increasingly heightened cyber environment that places demand on a higher level of operational resilience than before. While many actors have long had the capability to do significant harm, the shift in geopolitical dynamics has increased the likelihood that such capabilities may be used. Simultaneously, it has become easier for criminals to replicate advanced attacks, thus further broadening the range of actors able to carry out sophisticated operations.

This development reinforces the need for a strong and coordinated approach to resilience across the financial sector, ensuring that critical societal functions can continue even in extreme yet plausible scenarios.

For many years, the Danish financial sector has worked to strengthen their cyber and operational resilience, and progress has been made. The implementation of the Digital Operational Resilience Act (DORA) from 2025 will further strengthen cyber resilience for individual companies. Danmarks Nationalbank has placed priority on addressing cyber and other operational risks in close collaboration with the sector and with a sector wide approach due to high interconnectedness. Since 2016 this work has been anchored in the Financial Sector Forum for Operational Resilience (FSOR), which brings together key institutions and authorities under the Danmarks Nationalbanks's chairmanship to ensure a coordinated, sector-wide approach.

While this long-standing cooperation provides a strong foundation, today's threat landscape requires closer integration with Europe. Initiatives such as the ECB's Euro Cyber Resilience Board (ECRB) and the CIISI-EU information-sharing framework increasingly support cross-border situational awareness and coordinated responses demonstrating that operational resilience can be strengthened by collaborating across borders and sectors.

The current threat landscape also requires further strengthening of operational contingency measures. In December, Danmarks Nationalbank published an analysis assessing whether the financial activities most critical to society, i.e., for citizens, businesses and the public authorities, could be maintained if a central actor or system were to face an extreme yet plausible incident.

> The current threat landscape requires further strengthening of operational contingency measure.

The objective is hence to safeguard the most societally critical customer-facing functions such as access to deposits and account information, payments, and clearing of retail payments, but not to continue all activities for individual credit institutions. This distinction is important. While individual companies naturally focus on preserving their own operations, there must be contingency measures in place to ensure continuity of activities most critical to society to support the real economy and financial stability.

The analysis found that although the Danish financial sector shows high maturity, additional measures are needed to ensure continued access to critical customer data and basic payment activities if core systems or a critical actor become unavailable for an extended period. This reflects a shift in line with current threat landscape: Destructive cyberattacks, long-lasting outages or loss of data integrity can no longer be seen as unlikely edge cases.

The analysis led to a number of recommendations from Danmarks Nationalbank to key financial companies, aimed at enhancing emergency preparedness. Due to the interconnection of the financial sector, the focus was on initiatives where cross-sector collaboration is advantageous.

The recommendations included a bank emergency solution so that citizens can use payment cards, receive salaries and transfer money, and where businesses can receive customer payments and pay bills. The proposed bank emergency solution consists of centralised collection of critical customer deposit data in a secure data vault and the establishment of emergency platforms in the sector to ensure society access to basic banking services.

Looking ahead, strengthening emergency capabilities across the financial sector will require coordinated efforts nationally and in Europe. Nationally, sustained dialogue between authorities and financial companies is needed to implement emergency solutions for the most critical societal activities and ensure that these solutions are usable, tested and ready. At the European level, further cooperation and alignment will be highly beneficial.

Ultimately, strengthening operational resilience depends on ensuring that the financial system as a whole, not just individual companies, can continue delivering the critical services that citizens and businesses rely on, even when disruptions are severe.

NATHALY REY
Director, Google Cloud Regulatory Response – Google Cloud

The CTPP frontier: a paradigm shift in oversight

A new era has begun following the implementation of DORA and the designation of the first critical third-party service providers (CTPP). At Google Cloud, we take our role in the European financial ecosystem seriously and firmly believe that digital operational resilience is an essential foundation for systemic stability and sustainable innovation. We have welcomed DORA from its initial draft stages as an essential harmonization regulation designed to enhance the operational resilience of the European financial sector. In November 2025, Google Cloud EMEA was officially designated as a CTPP. We have prepared for this shift to direct oversight under DORA for many years with a dedicated readiness program, including the publication of numerous resources for our customers to support their own compliance.

DORA One Year Later: Our reflections

Reflecting on the first year of DORA, we observe that the industry is adopting a multi-pronged approach to cyber risks, focusing on technology adoption, enhanced risk management practices, and shifting from mere compliance to core governance responsibilities. DORA aims to bolster the European financial sector against ICT disruptions by standardizing incident reporting, resilience testing, and ICT third-party risk management. While it is still early days, we are confident that with robust stakeholder support and collaboration, digital operational resilience across the European financial sector will be significantly enhanced.

As we embrace direct oversight from the European Supervisory Authorities (ESAs) and our Lead Overseer, we are invested in continuing the constructive collaboration and supporting the oversight team in obtaining the necessary understanding of our organization. It is important to acknowledge that ICT providers, especially cloud service providers (CSPs), operate differently from traditional financial entities. For example, the cloud security shared responsibility model is critical to the cloud operating model.

The Imperative for International Cooperation

Because cyber threats and digital supply chains are inherently global, international cooperation is essential to manage systemic risks that span jurisdictions. This necessitates continuous cross-border information sharing and threat intelligence exchange.

> The recipe for a resilient future rests on three pillars: proper risk management that addresses dependencies, the rapid yet responsible adoption of AI, and a culture that can adapt as quickly as the threats it faces.

To prevent market fragmentation and drive efficiency in a global ecosystem, Google Cloud advocates for "regulatory interoperability". It is critical that frameworks like DORA, the UK Critical Third Party regime, and US oversight models are comparable and aligned in outcomes, even if they are not identical in text. Effective implementation of these frameworks requires effective collaboration amongst global financial services regulators to leverage existing supervisory insights and prevent conflicting mandates.

Leveraging Technology and AI for Operational Resilience

Technology, particularly Artificial Intelligence, has emerged as both a risk amplifier and a critical defensive necessity. Malicious actors are increasingly adopting AI tools to scale convincing phishing attacks, discover vulnerabilities, and create deep fakes designed to bypass Know-Your-Customer (KYC) security requirements.

Conversely, AI plays a paramount role in the fight against these evolving risks. AI solutions transform data analytics for faster decision-making, improve operational efficiencies, and drastically enhance risk detection. Tools like Google Cloud's Security Operations utilize AI to automate the triage of security alerts and detect subtle anomalies that human analysts might otherwise miss.

However, adopting AI effectively requires evolving a company's cybersecurity posture. Because AI models and agentic AI systems expand the surface area that needs protection, financial entities must harden existing data infrastructure, develop stringent access controls, and understand how these changes affect overall risk management. Supervised entities must pair their AI innovation with robust AI governance principles and a compliance-focused foundation to successfully mitigate risks and unlock this potential in the financial sector.

Conclusion

The first year of DORA's application marks a vital step toward a more secure, harmonized, and resilient European financial ecosystem. Operational resilience is not a destination but a continuous state of collaboration. The recipe for a resilient future rests on three pillars: proper risk management that addresses dependencies, the rapid yet responsible adoption of AI, and a culture that can adapt as quickly as the threats it faces. Google Cloud remains deeply invested in Europe's success and stands ready to operate as a trusted, transparent partner in this critical ongoing journey.

CARSTEN SCHMITT
Chief Financial Officer – Commerzbank AG

DORA as part of the overall resilience and cybersecurity framework

It has been a little more than one year since DORA became applicable in 2025. Since then, it has rightfully captured attention as the overarching framework for digital operational resilience in the financial sector – and beyond.

Yet, operational and cyber risk of the financial sector should be seen in the wider context of the economic ecosystem including financial sector clients and service providers. What brings all those actors together is not just the shared need to ensure resilience, but also the complexity of the regulatory framework they operate in. Regulatory requirements are introduced through DORA, the AI Act, the revised Network and Information Security Directive, the General Data Protection Regulation and the Cyber Resilience Act – not withstanding product-specific rules.

Some of those apply to entities, defining governance, roles and processes, while the application of others is based on the technology used or limited to certain products. The idea is clear: address risks and ensure that all gaps are closed.

But as it is often, the road to hell is paved with good intentions. The intent to close potential regulatory gaps has created a system that is characterised by overlaps and complexity. This is the case for the supervisory structure as well as procedures, e.g. for incident reporting. While DORA has created an end-to-end framework for digital operational resilience, focusing on more than just cybersecurity, financial institutions are still subject to a multitude of other rules, most of them coming with their own reporting requirements for incidents. All of them with different definitions, thresholds, templates, channels and timelines. This set-up forces financial institutions to stretch their resources between internal coordination and reporting, rather than enable them to focus on the actual management of the incident and its underlying root cause.

The AI Act brings additional supervisory authorities into the picture: Financial services authorities will be the relevant authorities for financial sector specific use cases, like creditworthiness assessments, but other, often horizontal authorities such as data protection authorities or the Bundesnetzagentur in Germany will be in charge for example for HR-related use cases. And this supervisory network is multiplied by the number of member states an entity is active in. Moreover, high-risk AI cases will need to be registered at the European Commission's AI Office. This increases the number of relevant stakeholders and bears the risk of potentially conflicting guidance, especially where the same AI system is used for different purposes.

Simplifying the operational resilience framework – move fast and break complexity.

The Digital Omnibus – real simplification?

The proposals of the Digital and AI Omnibus as part of the broader simplification agenda seek to address the complexity in the cyber resilience world and increase resilience. Unfortunately, the result will fall short of its goal and may in fact be the opposite of what's intended – at least for the financial sector.

The omnibus proposes a single-entry point for incident reporting across sectors and across different regulatory frameworks. What seems like a procedural simplification at first glance is expected to increase effort for financial institutions, because it will require re-engineering of the newly introduced DORA reporting systems. At the same time, the proposal does not foresee any changes to the reporting timelines or content. Overlaps between DORA and the Cyber Resilience Act are not addressed either. As ICT systems are covered under DORA, the need for an additional framework for products with digital elements is at least questionable. The legislators should use the opportunity to eliminate regulatory overlap and introduce a financial services exemption into the Cyber Resilience Act – similar to the ones already existing in the text.

The current proposals do not address supervisory complexity either. The AI omnibus picks up the most pressing issues related to the lack of detailed guidance for implementation and proposes a delayed applicability for high-risk use case requirements. This is highly welcome. Yet, the texts refrain from more structural changes. A clear allocation of supervision to sectoral authorities should at least be considered to increase legal certainty and free up resources on all sides as appropriate resourcing is the most promising way to increase resilience.